aveni

TRUST & SECURITY

TRUST & SECURITY

Built for financial services. Designed for trust.

At Aveni, trust is not a feature. It is the foundation of everything we build. Our platform is engineered to meet the standards of regulated financial institutions, where data sensitivity, compliance, and operational resilience are non-negotiable, giving you confidence that your data, your customers, and your business are protected.

ISO 27001 Certified

GDPR & UK GDPR Compliant

AWS AES-256 Encryption

Privacy by Design

FOUR PILLARS OF TRUST

01 · SECURITY

Security you can rely on

- **Data encryption.** Protected in transit with modern TLS and at rest with AES-256. Keys are managed securely and rotated regularly.
- **Secure cloud infrastructure.** Runs on AWS with encryption at rest everywhere. Each customer's data is isolated, with continuous monitoring and threat detection.
- **Access controls & 2FA.** Two-factor authentication is enforced on all accounts. Role-based permissions and logged, reviewed admin access limit who reaches your data.
- **Employee security & vetting.** Every employee is background-checked and bound by confidentiality. Devices are MDM-managed with disk encryption and anti-malware.

02 · COMPLIANCE

Built for regulated environments

- **ISO 27001 certified.** The globally recognised standard for information security management, independently validating our controls across the organisation.
- **GDPR & UK GDPR compliant.** Lawful basis, data subject rights, and purpose limitation are embedded into how we operate, protecting your customers at every step.
- **Audit-ready by design.** Clear traceability and documentation at every stage, supporting record keeping, Consumer Duty KPI monitoring, and FCA reporting.
- **Purpose-built for regulated firms.** Enables 100% call and document monitoring coverage across suitability, conduct, and customer vulnerability obligations.

03 · RESPONSIBLE AI

Responsible AI you can trust

- **No black boxes.** Activity traces, source citation, and decision logs give you clarity into how Aveni reached its conclusions, which is essential for regulated decisions.
- **Human oversight always.** Our tools support professionals, not replace them. Aveni surfaces intelligence and flags risk; final judgement always rests with your team.
- **Domain-specific models.** Our AI, including FinLLM, is trained for financial services, reducing hallucination risk and aligning outputs with your market.
- **Never used for training.** Customer and call data is never used to train our AI or any third-party provider's. This is enforced as a technical constraint, not policy alone.

04 · RESILIENCE

Operational resilience

- **High availability architecture.** Engineered for uptime and continuity, with redundancy built in at every level to minimise disruption and maintain service.
- **Backup & disaster recovery.** Robust backups and tested recovery plans protect against data loss, with automated deletion schedules under your control.
- **Incident response.** Clear, tested processes detect, respond to, and resolve security events quickly, with proactive communication to affected parties.
- **Continuous monitoring.** We proactively monitor for threats, vulnerabilities, and unusual activity, with all internal access logged and reviewed on a regular cadence.

DATA OWNERSHIP

Your data stays yours. Full stop.

We don't use your data to train general-purpose models, share it with third parties, or retain it beyond delivering our services to you, always in line with agreed terms and applicable regulations.

- Customer call data is never used to train Aveni's AI models
- Aveni only records meetings it is explicitly invited to join
- Conversations are private and accessible only to authorised users
- Third-party AI providers are never trained on your data
- You control what is recorded, what is shared, and when it is deleted
- Data is processed solely to deliver our services, and nothing else

"Your discussions often involve highly sensitive and confidential data. That is why privacy and security are not policy documents at Aveni. They're design requirements embedded into every product decision we make."

UNDER THE HOOD · FOR TECHNICAL & INFOSEC REVIEWERS

Your data. Protected.

ENCRYPTION

AES-256 at rest & in transit

Encryption applied across all AWS storage services, including all buckets and volumes. 256-bit AES end-to-end, with a regularly rotated root key removing long-term exposure.

AUTHENTICATION

2FA & role-based access

2FA enforced on all accounts. Internal admin access requires explicit security approval, restricted to job function, with all events logged and reviewed.

DEVICES

MDM & endpoint controls

All employee devices enrolled in mobile device management. Disk encryption enforced by default; anti-malware installed and centrally managed across the fleet.

PEOPLE

Vetted, bound employees

Every employee is background-checked and signs a confidentiality agreement. Access to customer environments is granted only on an explicit, approved operational need.

INFRASTRUCTURE

Isolated production

Customer data is logically separated by tenant within shared databases, buckets, and other AWS services, with complete isolation. No data from one customer is accessible to another.

DATA LIFECYCLE

Controlled retention

Users control their own data lifecycle. Conversations auto-purge after 30 days in trash; manual deletion is honoured immediately. No data persists beyond agreed terms.

COMMON QUESTIONS

Security & trust, answered

Are customer calls used to train Aveni's AI?

No. Customer call data, transcriptions, and related content are never used to train our AI or any third-party provider's. Data is processed solely to deliver the Aveni service, applied as a technical constraint, not just a contractual one.

How is data encrypted and where is it stored?

All data is stored across AWS with server-side encryption and 256-bit AES on all buckets and volumes. Keys use a regularly rotated root key; data in transit uses modern TLS. Each customer's data is logically separated by tenant, with no cross-customer access.

Who can access recordings and transcripts?

Only the account holder and people they explicitly authorise. Internal access requires security approval, is restricted to a specific operational need, and is fully logged. No customer data is accessible across organisation accounts.

How does Aveni support FCA & Consumer Duty?

Aveni enables 100% monitoring coverage of customer calls and documents, giving full oversight of conduct, complaints, suitability, and vulnerability risks, while automating monitoring, record keeping, and reporting to the standard regulators expect.

What happens when we delete data?

Deleted conversations move to Trash and are automatically purged after 30 days. Clearing them manually deletes immediately. No data persists beyond agreed retention terms or applicable regulatory requirements.

How is it controlled which meetings AI joins?

Aveni only records meetings it is explicitly invited to. Advisers control which meetings the bot attends during setup, changeable at any time. Recordings are clearly indicated to all participants, supporting consent and notification requirements.

What security certifications does Aveni hold?

ISO 27001 certification and full UK & EU GDPR compliance. Infrastructure runs on AWS with privacy-by-design principles across all development. Full certification documentation is available on request for due diligence.

Can we review documentation for due diligence?

Yes. Our team provides security documentation, answers technical questions, and supports your due diligence directly, with experience across information security questionnaires, vendor assessments, and procurement reviews.